EXHIBIT

A

VISA

Visa International Operating Regulations

15 October 2010

Cardholder and Transaction Information Security - U.S. Region

A U.S. Member must comply, and ensure that its Merchants and Agents comply, with the requirements of the Cardholder Information Security Program, available from Visa upon request or online at http://www.visa.com/cisp.

A third party that supports a loyalty program or provides fraud control services, as specified in "Disclosure of Visa Transaction Information - U.S. Region" and "Cardholder and Transaction Information Disclosure Limitations - U.S. Region," must comply with the requirements of the Cardholder Information Security Program.

A U.S. Member must comply, and ensure that its Merchants and Agents comply, with the Transaction Information security requirements in the *Visa International Operating Regulations*, the Payment Card Industry Data Security Standard (PCI DSS), and the validation and reporting requirements outlined in the Cardholder Information Security Program. The Payment Card Industry Data Security Standard (PCI DSS) and the Cardholder Information Security Program requirements are available online at http://www.visa.com/cisp.

An Acquirer must ensure that its Merchant:

- Implements and maintains all of the security requirements, as specified in the Cardholder Information Security Program
- Immediately notifies Visa, through its Acquirer, of the use of a Third Party
- Ensures that the Third Party implements and maintains all of the security requirements, as specified in the Cardholder Information Security Program
- Immediately notifies Visa, through its Acquirer, of any suspected or confirmed loss or theft of material or records that contain account information and:
  - Demonstrates its ability to prevent future loss or theft of account or Transaction information, consistent with the requirements of the Cardholder Information Security Program
  - Allows Visa, or an independent third party acceptable to Visa, to verify this ability by conducting a security review, at the Acquirer's own expense

ID#: 010410-010410-0008031

Fines and Penalties

Non-Compliance with Account and Transaction Information Security Standards VIOR 2.1.E

If Visa determines that a Member, its agent, or a Merchant has been deficient or negligent in securely maintaining the account or Transaction Information or reporting or investigating the loss of this information, Visa may fine the Member, as specified in the *Visa International Operating Regulations,* or require the Member to take immediate corrective action.

ID#: 010410-010410-0001753

Issuer Identification on Card

Visa identifies the Issuer that ordered the manufacture of a Visa Card or Visa Electron Card by either the name printed on the Visa Card or Visa Electron Card or the manufacturer product information printed on the back of the Visa Card or Visa Electron Card.

There is no time limit on a Member's right to reassign liability to the Issuer under this section.

ID#: 010410-010410-0008158

Counterfeit Card Transaction Reporting

If a Member discovers Counterfeit Card activity, the Member must immediately report the Account Number to Visa.

ID#: 010410-010410-0001816

Account Data Compromise Recovery (ADCR)

Account Data Compromise Recovery Process - U.S. Region

In the U.S. Region, the Account Data Compromise Recovery (ADCR) process allows Visa to determine the monetary scope of an account compromise event, collect from the responsible Member, and reimburse Members that have incurred losses as a result of the event.

ADCR allows the recovery of counterfeit transaction losses across all Visa-owned brands (i.e., Visa, Interlink, and Plus) when a violation attributed to another Visa Member could have allowed data to be compromised and the subsequent financial loss was associated with any of the following:

- A Visa Transaction
- An Interlink transaction
- A Plus transaction

This process is only available when there has been a violation of at least one of the following:

- Operating Regulations involving electronic storage of the full contents of any track on the Magnetic Stripe subsequent to Authorization of a Transaction
- Operating Regulations involving non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of the full contents of any track on the Magnetic Stripe
- Operating Regulations involving the PIN Management Requirements Documents that could allow a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization

The Account Data Compromise Recovery process includes:

- Counterfeit Fraud Recovery
- Operating Expense Recovery

ID#: 081010-010410-0000877

Transactions Excluded from ADCR Process - U.S. Region

In the U.S. Region, violations of the *Visa International Operating Regulations* not involving storage of Magnetic-Stripe Data are excluded from this process.

In the U.S. Region, violations not involving non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of the full contents of any track on the Magnetic Stripe are excluded from this process.

Violations not involving a Transaction are resolved as specified in "Visa Right to Fine" and as deemed appropriate by Visa.

ID#: 081010-010410-0000878

Determination of ADCR Eligibility - U.S. Region

Effective for Qualifying CAMS Events that occurred on or before 30 March 2009, following the fraud analysis and investigation of the compromise event, a U.S. Member:

- Is provided with findings in support of the preliminary determination that the event is eligible for the ADCR process
- Is provided with any estimated counterfeit fraud and operating expense liability amounts
- May submit a written appeal, within 30 calendar days of the preliminary findings notification date, with supporting documentation to Visa. Such appeal will be considered by the ADCR Review Committee or, if the total Acquirer liabilities are US $500,000 or more, the appeal will be considered by the Corporate Risk Committee. A determination of such appeal will be provided to the Acquirer.

Effective for Qualifying CAMS Events that occur on or after 31 March 2009, following the fraud analysis and investigation of the compromise event, the U.S. Member is provided with:

- Findings in support of the preliminary determination that the event is eligible for the ADCR process
- Any estimated counterfeit fraud and operating expense liability amounts

ID#: 010410-010410-0009035

Counterfeit Fraud Recovery Process - U.S. Region

A U.S. Member is compensated for a portion of its counterfeit fraud losses incurred as the result of a Magnetic-Stripe Data account compromise event. The Counterfeit Fraud Recovery process is initiated by Visa when:

- An account compromise event occurs
- A Compromised Account Management System (CAMS) Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members
- Effective for Qualifying CAMS Events that occur on or before 30 June 2010, the account compromise event involves at least 10,000 Account Numbers

- **Effective for Qualifying CAMS Events that occur on or after 1 July 2010,** the account compromise event involves at least 10,000 Account Numbers **and** a combined total of US $100,000 or more recovery for all Issuers involved in the event
- At least one of the following:
  - The full contents of any track on the Magnetic Stripe was stored subsequent to Authorization of a Transaction
  - A violation of the Payment Card Industry Data Security Standard (PCI DSS) could have allowed a compromise of the full contents of any track on the Magnetic Stripe
  - A violation of the PIN Management Requirements Documents could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization
- Incremental fraud is attributed to the particular account compromise event

ID#: 081010-010410-0000880

Counterfeit Fraud Reimbursement Conditions - U.S. Region

In the U.S. Region, only counterfeit fraud properly reported as specified in the *Visa International Operating Regulations* is considered when determining any reimbursement due.

ID#: 010410-010410-0000881

Baseline Counterfeit Fraud Level Determination - U.S. Region

In the U.S. Region, Visa determines a baseline counterfeit fraud level by analyzing reported Magnetic-Stripe-read counterfeit fraud losses that occurred up to 12 months before a Qualifying CAMS Event date and one month after the Qualifying CAMS Event date.

ID#: 010410-010410-0000882

Counterfeit Fraud Recovery Eligibility - U.S. Region

U.S. Members are eligible for Counterfeit Fraud Recovery when there is incremental counterfeit fraud activity above the baseline counterfeit fraud level, as determined by Visa.

ID#: 010410-010410-0000883

Counterfeit Card Recovery Process - U.S. Region

The U.S. Member deemed responsible for an account compromise event is notified of its estimated counterfeit fraud liability.

After the deadline for fraud reporting has passed, a Member communication broadcast is used to notify affected U.S. Members that an account compromise event qualifies for Counterfeit Fraud Recovery and advises them of their recovery amount.

The U.S. Member deemed responsible for the account compromise event is then notified of its actual counterfeit fraud liability.

ID#: 010410-010410-0008117

ADCR Reimbursement Guidelines - U.S. Region

The following rules are related to the recovery process in the U.S. Region:

- Only recovery amounts of US $25 or more are collected and distributed to affected U.S. Members.
- Only U.S. Members that were registered to receive CAMS Alerts at the time of the first CAMS Alert for the event that is the subject of the ADCR proceeding are eligible to receive counterfeit fraud reimbursement.
- Counterfeit fraud losses on Account Numbers that were included in a different Qualifying CAMS Event within the 12 months before the Qualifying CAMS Event date are excluded.
- If 2 or more Qualifying CAMS Events occur within 30 days of each other, and the events each involve a minimum of 100,000 Account Numbers, the responsible U.S. Members share liability for the counterfeit fraud amount attributed to the accounts in common.

ID#: 010410-010410-0000887

Counterfeit Fraud Liability Collection and Distribution - U.S. Region

Counterfeit fraud liability is collected from the responsible U.S. Member(s) through the Global Member Billing Solution. Funds are distributed the following month, at the Business ID level, through the Global Member Billing Solution, to affected Members.

ID#: 010410-010410-0000888

ADCR Administrative Fees - U.S. Region

In the U.S. Region, an administrative fee is charged to the Issuer for each reimbursement issued, as specified in the *Visa U.S.A. Fee Guide*.

ID#: 081010-010410-0000889

Operating Expense Recovery Process - U.S. Region

A U.S. Member enrolled in the Operating Expense Recovery process is compensated for a portion of its operating expenses incurred as a result of a Magnetic-Stripe Data account compromise event. The Operating Expense Recovery process is initiated by Visa when:

- An account compromise event occurs
- A CAMS Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members
- Effective for Qualifying CAMS Events that occur on or before 30 June 2010, the account compromise event involves at least 10,000 Account Numbers
- **Effective for Qualifying CAMS Events that occur on or after 1 July 2010**, the account compromise event involves at least 10,000 Account Numbers and a combined total of US $100,000 or more recovery for all Issuers involved in the event

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, in the U.S. Region, the appeal rights, as specified in "Enforcement Appeals - U.S. Region," are **not** applicable to ADCR.

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, Visa will notify the U.S. Member of the final disposition of the appeal.

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, in the U.S. Region, the decision on any appeal is final and **not** subject to any challenge.

Effective for Qualifying CAMS Events that occurred on or after 31 March 2009, Visa will collect from the U.S. Member an appeal fee, as specified in the *Visa U.S.A. Fee Guide,* through the Global Member Billing Solution. For a data compromise event that qualifies under both the ADCR process and the international Data Compromise Recovery solution, Visa will collect only one appeal fee from the Member, as specified in the *Visa U.S.A. Fee Guide.*

ID#: 081010-010410-0009036

Data Compromise Recovery Solution (DCRS)

Data Compromise Recovery Solution Overview

An Issuer of Visa International or Visa Europe may recover incremental counterfeit fraud losses resulting from a Data Compromise event involving theft of full Magnetic-Stripe Data under the Data Compromise Recovery solution from Member(s) to whom liability for such loss has been assigned pursuant to the Data Compromise Recovery solution.

ID#: 010410-010410-0003334

Data Compromise Recovery Solution Eligibility

Visa will determine a data compromise event, fraud, and Issuer eligibility under the Data Compromise Recovery Solution.

ID#: 010410-010410-0003335

Data Compromise Event Eligibility

Visa will determine data compromise event eligibility based on:

- Forensic confirmation or preponderance of evidence that a breach exists
- A violation of the Payment Card Industry Data Security Standard (PCI DSS) occurred that could allow a compromise of account data
- Full Magnetic Stripe counterfeit fraud occurred on a portion of exposed Account Numbers
- A minimum of 10,000 Account Numbers were exposed and a minimum of US $100,000 in Magnetic Stripe counterfeit fraud occurred during the data compromise event time period

ID#: 010410-010410-0000867

Data Compromise Fraud Eligibility Criteria

Visa will determine fraud eligibility based on all of the following:

- Counterfeit fraud was reported to Visa
- Authorized counterfeit fraud Transactions with full Magnetic-Stripe Data occurred, including Card Verification Value
- Counterfeit fraud Transactions occurred after the Magnetic-Stripe Data was exposed

ID#: 010410-010410-0000868

Unrecovered Counterfeit Fraud Losses

Visa will determine Issuer eligibility for unrecovered counterfeit fraud losses, based on the Issuer being:

- Capable of receiving Visa data compromise fraud alerts
- In compliance with regional Issuer fraud control programs

ID#: 010410-010410-0000869

Data Compromise Recovery Liability Time Limit

An Acquirer's liability under the Data Compromise Recovery solution is limited to a maximum time period of 13 months and is associated with a single data compromise event.

ID#: 010410-010410-0000870

Data Compromise Event Time Period

The data compromise event time period begins with the earliest known data exposure, not to exceed 12 months before the data compromise event alert and concludes 30 calendar days following the data compromise event alert.

ID#: 010410-010410-0000871

Data Compromise Fraud Loss Recovery

Issuers' total fraud loss recovery is limited to the:

- Maximum liability assigned to the Acquirer by Visa
- Amount recoverable from the Acquirer

ID#: 010410-010410-0000872